



PATENT APPLICATION  
Docket No. 8514-100

AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of: Ned Hoffman, et. al.

Serial No. 09/215,058 Examiner: James W. Myhre

Filed: December 17, 1998 Group Art Unit: 3622

For: TOKENLESS FINANCIAL ACCESS SYSTEM

Confirmation No. 7856

**TRANSMITTAL LETTER**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

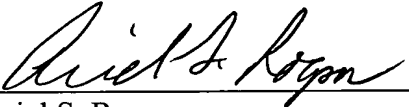
Enclosed for filing in the above-referenced application are the following:

- ☒ Reply Brief (in triplicate)
- ☒ Any deficiency or overpayment should be charged or credited to deposit account number 13-1703. A duplicate copy of this sheet is enclosed.


**Customer No. 20575**

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

  
Ariel S. Rogson  
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.  
1030 SW Morrison Street  
Portland, OR 97205  
503-222-3613

I hereby certify that this correspondence  
is being deposited with the United States  
Postal Service as first class mail in an  
envelope addressed to: Commissioner for  
Patents, P.O. Box 1450, Alexandria, VA  
22313-1450  
Date: July 18, 2005  
  
Christina Lawton



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Ned HOFFMAN, et al.

Serial No. 09/215,058

Examiner: James W. MYHRE

Confirmation No. 7856

Filed: December 17, 1998

Group Art Unit: 3622

For: **TOKENLESS FINANCIAL ACCESS SYSTEM**

Mail Stop Appeal Brief – Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**REPLY BRIEF**

**UNDER 37 C.F.R. § 41.41**

In the Examiner's Answer to the Appeal Brief filed May 16, 2005, the Examiner has presented six arguments in support of his earlier final rejection of the claims and responsive to Appellant's arguments presented in the Appeal Brief. These arguments are, in turn: that claim 21 of Houvener discloses using a biometric identifier in a first identification step; that Daugman discloses the use of iris identification for authorization of a commercial transaction; that it is old and well known to allow users to select names for their accounts; that Houvener discloses that when fraudulent activity is detected, the system is notified; that the user identification step in Houvener is complete after the comparison is made and that no information is sent between the computer system and the user or seller during this step; and that Examiner's arguments are not based on improper hindsight reasoning. These arguments are addressed in turn.

A. In section (11)(a) on pages 12-13 of the Examiner's Answer, the Examiner has argued that Houvener discloses using a biometric identifier as a single step in identifying a user by relying on claims 20 and 21 of Houvener. The Examiner attempts to support this argument by stating an example of a user entering a fingerprint as the first identification unit and having the system transmit the fingerprint to be compared against fingerprints on file.

The Examiner fails, however, to cite any part of Houvener that enables this type of transaction. That is because Houvener does not contain any description enabling one to use a biometric identifier to make a single step identification. The disclosure of Houvener only enables using biometric information to *verify* a previous identification.

The only way to enable Houvener is to use improper hindsight and reach into the Appellant's application to provide the necessary steps to complete a single-step identification using a biometric identifier.

The Examiner further argues that the second verification step in Houvener is a "superfluous" and "obvious" extension of Houvener's invention. Upon reading Houvener's "Summary of the Invention" at column 3, lines 14-15, the system of Houvener's "invention" is designed to provide "a system and method of *assessing the quality* of an identification transaction." (emphasis added). Note that the invention is not about providing an identification transaction but the verification of the quality of the identification already made. To modify Houvener as the Examiner has suggested would redesign the system of Houvener from the ground up. Houvener clearly teaches away from such a reading. For that reason, the second verification step in Houvener is necessary and not "superfluous", and cannot be omitted.

B. In section (11)(b) on page 13 of the Examiner's Answer, the Examiner has argued that Daugman discloses using a one-step process for identifying an individual for authorization of a commercial transaction. The Examiner relies on a mere passing mention of "other transaction authorizations" in Daugman as being a disclosure using iris identification to complete a commercial transaction.

First, the reference to "other transaction authorizations" made by Daugman is too vague to be considered a disclosure of using iris identification to complete a commercial transaction.

Second, as the Examiner noted, the Appellant argued in the initial Appeal Brief that Daugman neither discloses *nor enables* the use of iris identification to complete a commercial transaction. The Examiner fails to provide any argument regarding Daugman's lack of enablement. Possibly this is because Daugman does not contain a description enabling the use of iris identification to complete a commercial transaction. Again, the only way to enable Daugman is to use improper hindsight and to supplement Daugman with information from the Appellant's present application. That is impermissible.

C. In section (11)(c) on pages 14-15 of the Examiner's Answer, the Examiner has argued anew that "it is also old and well known to allow users (e.g. bank customers) to select names for their accounts." The Examiner has provided no documentation to corroborate this assertion. The Appellant disputes this brand new "Official Notice" and argues that it is not old to allow a user to select names for his or her accounts.

Further, the Examiner fails to answer the arguments put forth in the Appeal Brief that Examiners in other patents have specifically allowed claims including the account index code. As an example, in Applicant's U.S. Patent Application Serial No. 09/731,536, filed December 6, 2000, currently allowed, the Examiner specifically indicated that the use of an account index code provided a distinguishing feature over prior art. Another example is Applicant's U.S. Patent Application Serial No. 09/879,370, now U.S. Patent No. 6,662,166. The Appellant is not asserting that the use of an account index code by itself is new, but that the combination of the account index code with tokenless biometric identification for commercial transactions is novel and non-obvious.

D. In section (11)(d) on pages 15-16 of the Examiner's Answer, the Examiner argues with respect to claim 11 that Houvener "discusses numerous ways to prevent fraud by the user and to notify the system when suspected fraudulent activity occurs" (citing column 6, line 52 through column 7, line 44; column 8, line 42 through column 9, line 4; and column 11, lines 10-24). The Examiner argues that these methods would detect when a user is attempting to re-register. The Examiner further argues the methods could perform other tasks not at issue with claim 11.

As stated in the Appeal Brief, the Examiner is arguing from general comments made in Houvener, without addressing the specifics of claim 11 of the present application. Column 6, lines 52-67 discuss the problem of identity-based fraud with reference to identification documents that are susceptible to forgery. Column 7, lines 38-42 discusses other identity-based fraud indicators, and specifically mentions the possibility of "an individual enrolling an abnormally large number of accounts . . . in a short period of time or . . . under different names using a common address." While this excerpt describes one technique to recognize a user registering multiple times with the system, it is by no means the only way to recognize such an occurrence, and it is not the claimed invention.

Column 11, lines 10-24 describes situations having no relationship to the language of claim 11. Here, Houvener describes user transactions occurring at geographically distant points at the same time. This section does not disclose detecting the re-registration of a user.

To take a general comment about fraud, interpret it to mean that there is a need to watch for re-registration in all circumstances, and use that interpretation to reject any and all other techniques to identify re-registration misinterprets the language of Houvener.

Finally, as stated in the Appeal Brief, the fraud that Houvener is concerned about is a single individual enrolling a number of accounts, not repeated entry of *a single biometric*. Claim 11 recognizes that a single user might legitimately register a number of accounts: note that claim 1, from which claim 11 depends, indicates that the user “registers . . . at least one user financial account”: at least one, and possibly more. Claim 11, in contrast with Houvener, is concerned with the situation where a user has previously registered with the system, and now attempts to register anew, using the same biometric. The situations addressed by Houvener and the claimed invention are very different, and neither suggests the other.

Finally, the Examiner has stated that “[t]he Examiner assumes that the Appellant is alerting the system when a user is attempting to re-register the *same* accounts also, not just adding *new* accounts under his identity” (Examiner’s Answer dated May 16, 2005, section (11)(d) on page 15; emphasis in original). The Applicant agrees that a user might want to add new accounts under an already-registered biometric, which would not be re-registration. But re-registration is not limited to the situation where a user attempts to register a previously-registered biometric along with the same accounts. For example, consider the situation where an identity thief has registered a particular biometric with some user’s account. The identity thief (assuming the wrongness of his actions does not affect him) will eventually attempt to steal someone else’s account and attempt to register it. Adding the new account to the previously-registered biometric simply puts more evidence in the same place, so the thief would prefer to avoid doing so. The thief would therefore want to set up a new “identity” to take advantage of the new account. This would involve registering a new biometric, and associating the newly stolen account number with the new registration. But if the thief re-registers an existing biometric, this re-registration should be prevented.

Thus, the Examiner’s assumption is not warranted. Re-registration as described in claim 11 is directed toward a user registering the same biometric more than once, but not limited to situations where the user is attempting to register the same accounts. Because the Examiner has made a false assumption in rejecting the claims and this false assumption is made for the first time in the Examiner’s Answer, the Examiner has effectively read a non-existent limitation into the claims, and the rejection is therefore inappropriate.

E. In section (11)(e) on page 16 of the Examiner's Answer, the Examiner argues that the user identification step is complete after the comparison of bid biometric with registration biometric samples and that no information is sent between the computer system and the user or seller during this step.

Houvener does not disclose nor enable using biometric information to identify a user in a single step. As explained above in section A, beyond a passing mention in claim 21, Houven does not disclose a single step identification system that uses biometric information as an initial identifier. Further, Houven does not enable a single step identification system that uses biometric information as in an initial identifier because Houven contains no description at all as to how this would be accomplished.

Houvener is directed toward improving the assessment of an identification already made by utilizing biometric information make that assessment. Further, Houven teaches the need for verification. Houven solves the verification need by sending biometric information back to the seller who uses that biometric information to confirm an identification.

As Applicant has argued above, identification according to the claimed invention is a single-step process and is complete without transmitting any information from the computer system to the user or seller. The implication of this statement is that after the single-step identification, the user's identity is not only known, but the system trusts the identification to be correct. The identification via biometric comparison is itself trustworthy. In other words, verification is not needed in the claimed invention.

Houvener imposes the verification step because Houven does not trust that the identification step was correct. This is made clear by the first sentence of Houven: "Positive identity *verification* is critical . . . ." (column 1, line 32; emphasis added). In other words, Houven takes as given that identification without verification is not trustworthy. For commercial entities to implement Houven as the Examiner has proposed returns the commercial entities to the original level of risk that existed before Houven.

Therefore, it is incorrect to say that "the user identification step in Houven is complete after the comparison has been made and no information is sent between the computer system and the user or seller during this step" (Examiner's Answer dated May 16, 2005, section (11)(e), page 16). Verification of the user's identity is critical to the Houven system, because the user's identity cannot be trusted in Houven until after "verification" is complete. To say that identification and verification are separate concepts and that

verification can be skipped would leave sellers using the Houvener system no better off from a risk perspective than they were before Houvener.

Consider also the implications of the Examiner's reasoning. If the Examiner were correct – in other words, identification and verification were separate concepts, and verification could be omitted – a user could provide a number, such as a driver's license number or a social security number (*see* column 9, lines 36-39 of Houvener). That number is then used to "identify" the user. Since verification is not needed, the user is now completely identified. As should be clear, this process would provide a seller no more security that the user is who he says he is than would be available without Houvener. Clearly, the Examiner's reasoning is flawed.

The Examiner might argue that this example does not rely on the first identification unit being a biometric identification unit. But, as argued above, Houvener does not enable the first identification unit being a biometric identification unit. Further, regardless of how the Examiner argues the system would work with a biometric identification unit as the first identification unit, the system must work the same way even if the first identification unit is not a biometric. For the Examiner to argue that Houvener operates one way when the first identification unit is a biometric identification unit and another way when the first identification unit is not a biometric identification unit completely rewrites Houvener and ignores what Houvener specifically teaches. Thus, Houvener teaches away from the Examiner's suggestion that verification is not necessary to complete identification of the user. And because Houvener requires this second step, which involves sending information between the computer system and the user or seller during this step, Houvener teaches away from the features of the claimed invention.

F. In section (11)(f) on page 17 of the Examiner's Answer, the Examiner argues that improper hindsight was not used and that the initial identification step of Houvener is accomplished using substantially the same methods as the present application.

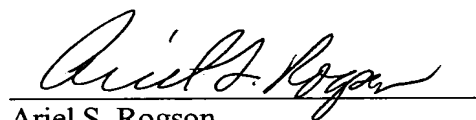
Houvener does not enable one to use a single step identification process using a biometric identifier. Houvener teaches and enables making an initial identification and then using biometric information to verify the initial identification. Houvener does not describe any way to accomplish using biometric information to complete the initial transaction. The Examiner relies solely on the language of Houvener's claim 21 to support using the biometric identification unit as the first identification unit. But the Examiner's interpretation of claim 21 is not enabled by the Houvener specification. Thus, the Examiner is using

improper hindsight to reject the claims because this improper hindsight is needed to enable Houvener to perform a single step identification using a biometric sample.

In conclusion, the rejections should be reversed because: Houvener and Daugman do not teach or suggest identification using a biometric, identification to complete a commercial transaction, permitting users to select names for their accounts, detecting re-registration of a biometric, or identification being complete after comparison of the bid biometric with no information sent between the computer system and the user or seller after comparison of the bid biometric, and the Examiner was using improper hindsight in rejecting the claims.

For the foregoing reasons, Appellant requests that the Board reverse the Examiner's rejections to Appellant's claims.

Respectfully submitted,  
MARGER JOHNSON & MCCOLLOM, P.C.



Ariel S. Rogson  
Registration No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.  
1030 S.W. Morrison Street  
Portland, Oregon 97205  
(503) 222-3613

I hereby certify that this correspondence  
is being deposited with the United States  
Postal Service as first class mail in an  
envelope addressed to: Commissioner for  
Patents, P.O. Box 1450, Alexandria, VA  
22313-1450  
Date: July 18, 2005

  
Christina Lawton